UNITED STATES DISTRICT COURT
EASTERN DISTRICT OF MICHIGAN
SOUTHERN DIVISION

CHRIS KEY, Individually and on Behalf of All Others Similarly Situated, Plaintiff, v. FLAGSTAR BANK, FSB, Defendant.	No. 2:22-cv-12689 CLASS ACTION COMPLAINT **JURY TRIAL DEMANDED**

Plaintiff Chris Key, individually and on behalf of all others similarly situated, brings this class action against Flagstar Bank, FSB ("Flagstar" or "Defendant"). Plaintiff makes the following allegations, except as to allegations specifically pertaining to Plaintiff, upon information and belief based upon, *inter alia*, the investigation of counsel and review of public documents.

NATURE OF THE ACTION

1. This is a putative class action on behalf of the over 1.5 million individuals whose sensitive personal identifying information ("PII") was compromised in a cybersecurity breach of Flagstar, which was announced on or about June 17, 2022 (the "Flagstar Breach").

2. Flagstar's reports of the Flagstar Breach to several state attorneys general revealed that the compromised PII consisted of names, addresses, Social

KELLER ROHRBACK L.L.P.
1201 THIRD AVENUE, SUITE 3200
SEATTLE, WA 98101-3052
TELEPHONE: (206) 623-1900
FACSIMILE: (206) 623-3384

Security numbers, financial information (e.g. account numbers, credit or debit card numbers), and "other" types of PII.

3. Flagstar failed to adequately protect consumers' sensitive PII, providing a means for unauthorized intruders to access Flagstar's computer network and steal sensitive PII. With access to someone's PII, it is possible to misuse that person's name to do some or all of the following: take out loans; open new financial accounts; obtain government benefits; file a fraudulent tax return and obtain a tax refund; obtain a driver's license or identification card; or give false information to police during an arrest.

4. As a result of the Flagstar Breach, Plaintiff and Class members have been exposed to a heightened and imminent risk of fraud and identity theft. Plaintiff and Class members must now, and in the future, closely monitor their financial accounts to guard against identity theft. Plaintiff and Class members may be faced with fraudulently incurred debt. Plaintiff and Class members may also incur out of pocket costs for, among other things, obtaining credit reports, credit freezes, or other protective measures to deter or detect identity theft.

5. Plaintiff seeks to remedy these harms on behalf of themselves and all similarly situated individuals and entities whose sensitive personal identifying information was accessed during the Flagstar Breach.

6. Plaintiff seeks remedies including, but not limited to, reimbursement of out-of-pocket losses, further credit monitoring services with accompanying identity theft insurance, and improved data security.

JURISDICTION AND VENUE

7. Venue is proper in this District pursuant to 28 U.S.C. § 1391(b)(1) & (2) because Flagstar is headquartered in this District, and because a substantial part of the events giving rise to these claims occurred in and emanated from this District.

8. This Court has general personal jurisdiction over Flagstar because it is a resident and citizen of Michigan and conducts substantial business in this District.

9. This Court has subject-matter jurisdiction pursuant to the Class Action Fairness Act, 28 U.S.C. § 1332(d) because the amount in controversy exceeds the sum or value of $5,000,000, exclusive of interest and costs. In addition, the action is a class action; there are members of the proposed Class who are diverse from Defendant; and there are more than 100 proposed Class members. This Court has supplemental jurisdiction over state law claims pursuant to 28 U.S.C. § 1367 because they form part of the same case or controversy as the claims within the Court's original jurisdiction.

PARTIES

10. Plaintiff Chris Key is a resident and citizen of Wichita Falls, Texas.

11. Plaintiff opened a Flagstar mortgage account in 2010 and opened an emergency credit card account in approximately 2018. Plaintiff received a letter in the summer of 2022 from Flagstar notifying him that his PII had been compromised.

12. Flagstar serves customers throughout the United States. Defendant Flagstar Bank, FSB is a Michigan-based entity with its principal place of business at 5151 Corporate Drive, Troy, Michigan 48097. Defendant is a full-service bank that provides commercial, small business, and consumer banking services, as well as home loans.

FACTUAL ALLEGATIONS

I. Flagstar

13. Flagstar Bank, FSB ("Flagstar") is a federal savings bank and the seventh-largest bank mortgage originator in the nation. It operates over 150 branches in Michigan, Indiana, California, Wisconsin, and Ohio, and its mortgage division operates nationally through retail locations and a wholesale network of third-party mortgage originators. Handling recordkeeping for over $300 billion in home loans, Flagstar is a leading servicer and subservicer of mortgage loans.

14. Among its Guiding Principles, Flagstar "believe[s] that banking with us will always be personal, private, and secure." This isn't the case.

15. Defendant's privacy policy states that it takes steps to keep Personal Identifying Information ("PII") safe and secure:

> To protect your personal information from unauthorized access and use, we use security measures that comply with federal law. These measures include computer safeguards and secured files and buildings.[1]

16. Additionally, Defendant's Privacy Statement specifically states:

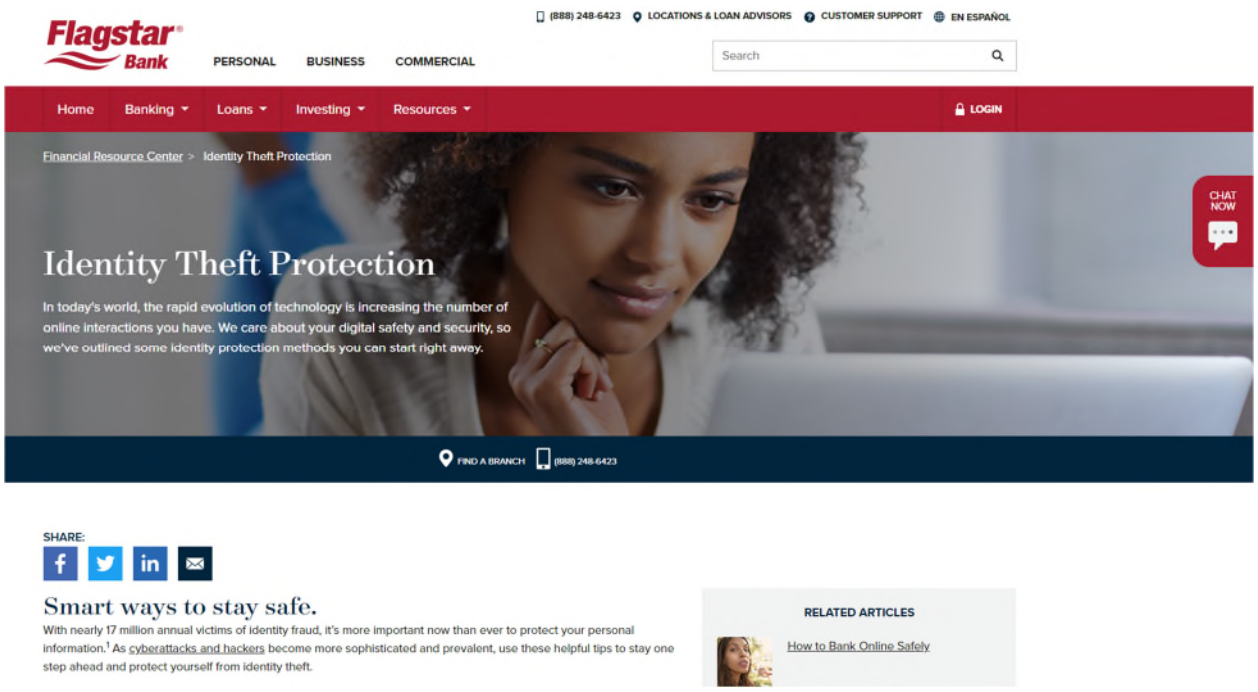
> Flagstar is committed to maintaining the security of the data you provide us. We use security controls that comply with applicable federal laws to protect against unauthorized access and use of your Personal Information in our custody or control. These measures may include computer safeguards and secured files and buildings. While we are focused on the security of your Personal Information, you must remember that the Internet is a global communications vehicle open to threats, viruses, and intrusions from others. For this reason, Flagstar cannot promise, and you should not expect, that we will be able to protect your Personal Information at all times and in all circumstances. Flagstar cannot guarantee the security and privacy of transmissions via the Internet, and we will not be liable for any lack of security relating to the use of the Banking Services by you. You agree that you will not hold Flagstar liable for any damages resulting from any loss of privacy or security occurring in connection with any such communications.[2]

17. Defendant highlights the importance of identity theft protection on its website, reassuring customers it "care[s] about [their] digital safety and security,"

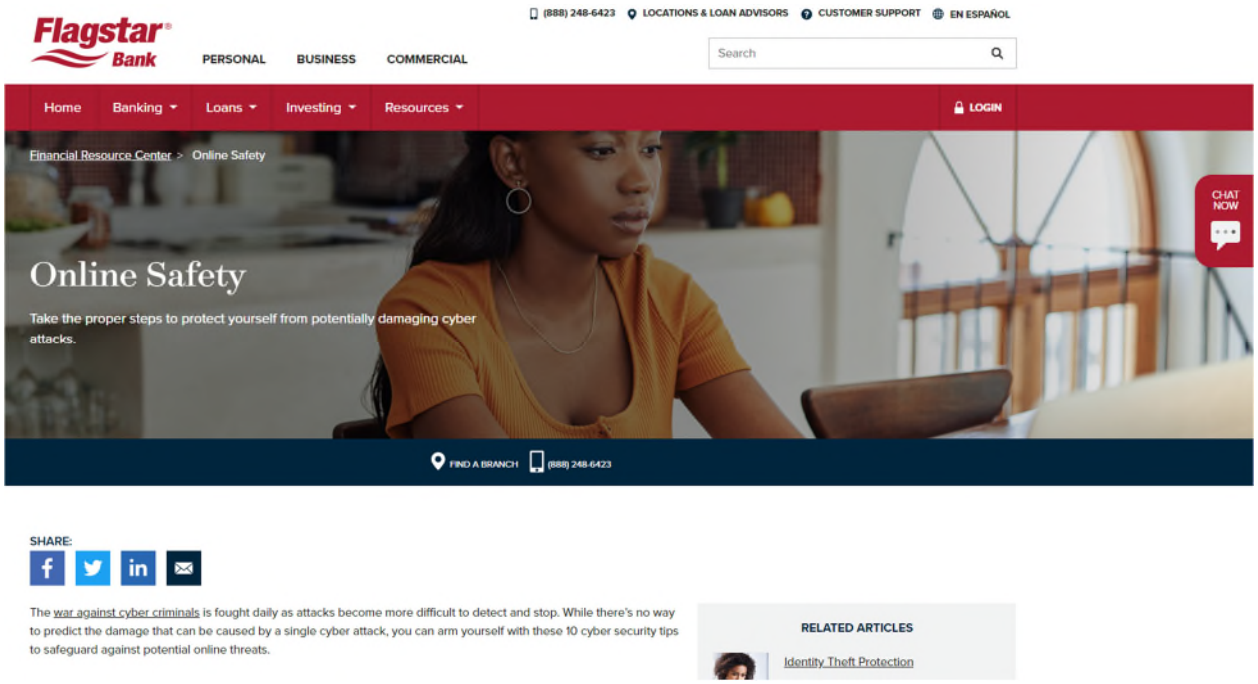
[1] Flagstar Bank, *About Your Privacy*, Rev. (02/2018), https://www.flagstar.com/content/dam/flagstar/pdfs/about-flagstar/PrivacyPolicy.pdf.

[2] Flagstar Bank, *Privacy Statement*, https://www.flagstar.com/legal-disclaimers/privacy-statement.html#6.

instructing them on "smart ways to stay safe," and saying "…it's more important now than ever to protect your personal information."



18. Defendant further highlights the importance of online safety and danger of cyberattacks on its website, telling customers "Take the proper steps to protect yourself from potentially damaging cyber attacks."



II. The Data Breach

19. On or about June 17, 2022, Flagstar notified the Maine Attorney General's Office that it had experienced a cybersecurity breach between December 3, 2021 and December 4, 2021 that included customers' names or other personal identifying information in combination with Social Security numbers. Flagstar reported that the breach had been discovered approximately six months later on June 2, 2022, and that 1,547,169 individuals were affected.

20. Flagstar also reported that affected individuals were sent a written notification of the breach on June 17, 2022 and would be offered two years of credit monitoring and identity repair services through Kroll.

21. A few days later, on or about June 20, 2022, Flagstar notified the Texas Attorney General's Office that it had suffered the Flagstar Breach. Flagstar's

notification to the Texas Attorney General revealed that names, addresses, Social Security numbers, financial information, and "other" information had been affected by the Flagstar Breach.

22. However, Flagstar informed multiple media outlets that it had learned of the breach in December 2021. In a statement to CNET, Flagstar represented that it had detected the intrusion "right away," but had delayed disclosing the breach until it had completed its investigation. Flagstar also admitted to PC Mag that it "detected and contained the incident in December 2021."

23. Despite knowing about the Flagstar Breach in December 2021, Flagstar delayed notifying customers whose personal information had been compromised until Flagstar sent a letter to affected individuals on or about June 17, 2022.

24. The Flagstar Breach was not the first time Flagstar customer data was the subject of a cybersecurity breach. Less than a year earlier, in January 2021, hackers gained unauthorized access to Flagstar customer names, Social Security numbers, and home addresses through a breach of third-party vendor Accellion's computer systems. The January 2021 breach put Flagstar on notice that its systems were likely to be targeted by hackers seeking to obtain personal identifying information.

25. Despite this knowledge, Flagstar failed to implement and maintain reasonable security procedures and practices appropriate to the nature of the information to protect its customers' personal information.

26. Flagstar also failed to adopt adequate protective measures to ensure that consumers' sensitive personal identifying information would not be improperly accessed.

27. As a result of Flagstar's inadequate measures, sensitive personal identifying information relating to at least 1.5 million individuals was obtained from Flagstar's computer network.

28. As a result of Defendant's failure to keep their personal identifying information from unauthorized access, Plaintiff and Class members are in imminent, immediate, and continuingly increased risk of harm from fraud and identity theft.

29. Plaintiff and Class members face a present and substantial risk of out-of-pocket fraud losses such as loans opened in their names, government benefits fraud, tax return fraud, utility bills opened in their names, credit card fraud, and similar identity theft.

30. Additionally, Plaintiff and Class members face a present and substantial risk of being targeted for future phishing, data intrusion, and other illegal schemes based on their personal identifying information.

31. As a condition of providing services to its customers, Defendant requires that its customers entrust Defendant with highly confidential personal information.

32. By obtaining, collecting, and storing the Plaintiff's and Class members' personal information, Defendant assumed legal and equitable duties and knew, or should have known, that it was responsible for protecting the personal information from disclosure.

33. Plaintiff and Class members have taken reasonable steps to maintain the confidentiality of their personal information and relied on Defendant to keep their personal information confidential and securely maintained, to use this information for business purposes only, and to make only authorized disclosures of this information.

34. Defendant's negligence in safeguarding Plaintiff's and Class members' personal information is further exacerbated by the data breach it experienced in January of 2021.

35. Despite the Defendant's recent previous data breach and the prevalence of public announcements of data breach and data security compromises, Defendant failed to take appropriate steps to protect the personal information of Plaintiff and Class members from being compromised.

36. To make matters worse, Defendant has offered inadequate services in wake of the Flagstar Breach. Flagstar is offering identify theft monitoring, including credit monitoring, fraud consultation, and identity theft restoration. Defendant places the burden on Plaintiff and Class members by requiring them to expend the time to enroll in these services, instead of automatically enrolling all those impacted by the Flagstar Breach. Moreover, Flagstar is only offering identity monitoring services for two years, even though the ramifications of personal identifying theft can extend far beyond two years.

37. Flagstar has taken minimal steps to notify customers of the breach. On information and belief, on or around June 17, 2022—over six months after the Flagstar Breach occurred—Flagstar sent a short letter to certain customers notifying them that the breached data included their personal information and posted a terse notification on its website, stating:

> How to Protect Your Information: June 17, 2022
> In December 2021, Flagstar experienced a cyber incident that involved unauthorized access to our network. We want to take a moment to detail what happened, what this means for you, and how you can protect your information.
>
> What happened?
> Upon learning of the incident, we promptly activated our incident response plan, engaged external cybersecurity professionals experienced in handling these types of incidents, and reported the matter to federal law enforcement. We continue to operate all services normally.

Since then, we have taken several measures to toughen our information security. We now believe we have strengthened processes and systems in a way that should reduce our cyber vulnerabilities in the future.

What is Flagstar doing?
On June 2, 2022, we concluded an extensive forensic investigation and manual document review. We are in the process of notifying individuals who may have been impacted directly via U.S. Mail to extend complimentary credit monitoring services.

For those impacted, we have no evidence that any of your information has been misused. Nevertheless, out of an abundance of caution we have secured the services of Kroll to provide identity monitoring at no cost to you for two years.

If you have already activated identity monitoring services through Kroll offered to you previously by Flagstar, we are offering an extension of your services for an additional two years. To enroll in the extension, please call (855) 503-3384 and a representative will assist you with the extension.

Flagstar has also established a call center dedicated to handling inquiries related to this incident and to help impacted individuals take advantage of their identity protection services, which can be reached at (855) 503-3384 between the hours of 9:00am – 6:30pm ET, Monday through Friday. If you are not an impacted individual, but you have questions about how to keep your information safe, please read the following article which provides helpful tips and guidance.[3]

[3] Customer Data Information Center, *How to Protect Your Information: June 17, 2022*, FLAGSTAR BANK (June 17, 2022), https://www.flagstar.com/customer-support/customer-data-information-center.html.

V. Industry Standards for Data Security

38. The U.S. Federal Trade Commission ("FTC") publishes guides for businesses for cybersecurity[4] and protection of PII[5] which includes basic security standards applicable to all types of businesses.

39. The FTC recommends that businesses:

a. Identify all connections to the computers where you store sensitive information;

b. Assess the vulnerability of each connection to commonly known or reasonably foreseeable attacks;

c. Do not store sensitive consumer data on any computer with an internet connection unless it is essential for conducting their business;

d. Scan computers on their network to identify and profile the operating system and open network services. If services are not needed, they should be disabled to prevent hacks or other potential security problems. For example, if email service or an internet connection is not necessary on a

[4] Start with Security: A Guide for Business, FTC (June 2015), https://www.ftc.gov/system/files/documents/plain-language/pdf0205-startwithsecurity.pdf.

[5] Protecting Personal Information: A Guide for Business, FTC (Oct. 2016), https://www.ftc.gov/system/files/documents/plain-language/pdf-0136_proteting-personal-information.pdf.

certain computer, a business should consider closing the ports to those services on that computer to prevent unauthorized access to that machine;

e. Pay particular attention to the security of their web applications—the software used to give information to visitors to their websites and to retrieve information from them. Web applications may be particularly vulnerable to a variety of hack attacks;

f. Use a firewall to protect their computers from hacker attacks while it is connected to a network, especially the internet;

g. Determine whether a border firewall should be installed where the business's network connects to the internet. A border firewall separates the network from the internet and may prevent an attacker from gaining access to a computer on the network where sensitive information is stored. Set access controls—settings that determine which devices and traffic get through the firewall—to allow only trusted devices with a legitimate business need to access the network. Since the protection a firewall provides is only as effective as its access controls, they should be reviewed periodically;

h. Monitor incoming traffic for signs that someone is trying to hack in. Keep an eye out for activity from new users, multiple log-in attempts from unknown users or computers, and higher-than- average traffic at unusual times of the day; and

i. Monitor outgoing traffic for signs of a data breach. Watch for unexpectedly large amounts of data being transmitted from their system to an unknown user. If large amounts of information are being transmitted from a business' network, the transmission should be investigated to make sure it is authorized.

40. Defendant was entrusted with its customers' PII and had a duty to those customers to keep their PII secure.

CLASS ALLEGATIONS

41. Plaintiff brings this class action pursuant to Fed. R. Civ. P. 23 on behalf of the following class:

> All individuals and entities in the United States whose personal identifying information was accessed in the cybersecurity breach announced by Flagstar on or about June 17, 2022 (the "Nationwide Class").

42. Excluded from the class are Flagstar; any parent, subsidiary, or affiliate of Flagstar or any employees, officers, or directors of Flagstar; legal representatives, successors, or assigns of Flagstar; and any justice, judge, or magistrate judge of the United States who may hear the case, and all persons related to any such judicial officer, as defined in 28 U.S.C. § 455(b).

43. Upon information and belief, the Nationwide Class consists of over a million geographically dispersed members, the joinder of whom in one action is

impracticable. Disposition of the claims in a class action will provide substantial benefits to both the parties and the Court.

44. Flagstar's uniform wrongful actions and/or inaction violated the rights of each member of the Nationwide Class were violated in a similar fashion.

45. The following questions of law and fact are common to each Class member and predominate over questions that may affect individual Class members:

a. whether Flagstar engaged in the wrongful conduct alleged herein;

b. whether Flagstar was negligent in collecting, storing, and/or safeguarding the sensitive personal identifying information of the Class members;

c. whether Flagstar owed a duty to Plaintiff and Class members to adequately protect their personal information;

d. whether Flagstar breached its duties to protect the personal information of Plaintiff and Class members;

e. whether Flagstar knew or should have known that its data security systems and processes were vulnerable to attack;

f. whether Flagstar's conduct proximately caused damages to Plaintiff and Class members;

g. whether Plaintiff and Class members are entitled to equitable relief including injunctive relief; and

h. whether the Class members are entitled to compensation, monetary damages, and/or any other services or corrective measures from Flagstar, and, if so, the nature and amount of any such relief.

46. Plaintiff's claims are typical of the claims of the Nationwide Class in that Plaintiff, like all Class members, had his sensitive personal identifying information compromised in the Flagstar Breach.

47. Plaintiff is committed to the vigorous prosecution of this action and will fairly and adequately represent and protect the interests of the proposed Nationwide Class. Plaintiff has no interests that are antagonistic to and/or that conflict with the interests of other putative Class members.

48. Plaintiff has retained counsel competent and experienced in the prosecution of complex class action litigation.

49. The members of the proposed Nationwide Class are readily ascertainable.

50. A class action is superior to all other available methods for the fair and efficient adjudication of the claims of the Nationwide. Plaintiff and the Class members have suffered (and continue to suffer) irreparable harm because of Flagstar's conduct. The damages suffered by some of the Class members may be

relatively small, preventing those Class members from seeking redress on an individual basis for the wrongs alleged herein. Absent a class action, many Class members who suffered damages because of the cybersecurity breach of Flagstar will not be adequately compensated.

51. Prosecuting separate actions by individual Class members would create a risk of inconsistent or varying adjudications that would establish incompatible standards of conduct for Flagstar. Additionally, adjudications with respect to individual Class members, such as adjudication as to injunctive relief, as a practical matter, would be dispositive of the interests of the other Class members not parties to the individual adjudications or would substantially impair or impede their ability to protect their interests.

CAUSES OF ACTION

COUNT I
NEGLIGENCE
(on behalf of the Class)

52. Plaintiff repeats and re-alleges each and every allegation set forth above as if fully set forth herein.

53. Defendant had a duty to Class members to exercise reasonable care in safeguarding and securely maintaining Class members' personal information. Defendant's duty included a responsibility to implement systems and processes by

which it could detect and prevent a breach of its security systems in a timely manner and, in the case of a breach, to give prompt notice to those affected.

54. Defendant owed a duty of care to Class members to provide data security consistent with industry standards and other requirements and to ensure that its systems, networks, and the personnel responsible for them adequately safeguarded and maintained Class members' personal information.

55. It was reasonably foreseeable to Flagstar that a breach of security was likely to occur given the known frequency of ransomware attacks and data breaches. It was therefore reasonably foreseeable that Flagstar's failure to adequately safeguard Class members' private information would cause damage to the Nationwide Class as alleged herein.

56. Defendant, by and through its negligent acts and/or omissions, breached its duties to Class members by failing to exercise reasonable care in safeguarding and securely maintaining Class members' sensitive personal identifying information within its possession, custody and control. Defendant further breached its duties to Class members by failing to disclose the Flagstar Breach in a timely manner or notify Class members that their sensitive personal identifying information had been, or was believed to be, compromised.

57. But for Defendant's negligent and wrongful breach of its duties to Plaintiff and Class members, the Flagstar Breach would not have occurred, and Class members' sensitive personal information would not have been compromised.

58. Class members' substantial injuries are a direct and proximate result of Defendant's negligence.

COUNT II
NEGLIGENCE PER SE
(on behalf of the Class)

59. Plaintiff repeats and re-alleges each and every allegation set forth above as if fully set forth herein.

60. Pursuant to Section 5 of the Federal Trade Commission Act, 15 U.S.C. § 45, "unfair. . . practices in or affecting commerce" including, as interpreted and enforced by the FTC, the unfair act or practice of failing to use reasonable measures to protect sensitive personal identifying information are prohibited. Pursuant to that Act, Defendant had a duty to use reasonable measures to protect Class members' sensitive personal identifying information and to provide fair data security practices and computer systems to safeguard Class members' sensitive private information.

61. By failing to have reasonable data security measures in place, Defendant engaged in an unfair act or practice within the meaning of and in violation of Section 5 of the FTC Act.

62. Flagstar's violation of Section 5 of the FTC Act constitutes negligence per se.

63. The Flagstar Breach and the substantial injuries Plaintiff and Class members suffered as a direct and proximate result of the breach were reasonably foreseeable consequences of Defendant's negligence per se.

COUNT III
VIOLATION OF TEXAS DECEPTIVE TRADE PRACTICES-CONSUMER PROTECTION ACT
(Texas Bus. & Com. Code § 17.41 *et seq*.)
(on behalf of the Class)

64. Plaintiff repeats and re-alleges each and every allegation set forth above as if fully set forth herein.

65. The Texas Deceptive Trade Practices-Consumer Protection Act ("DTP"), Texas Bus. & Com. Code § 17.41, *et seq.*, protects consumers from false, misleading or deceptive acts or practices, unconscionable actions, and breaches of warranty.

66. Plaintiff is a "consumer" as defined by Tex. Bus. & Com. Code § 17.45(4).

67. Defendant is a "person," as defined by Tex. Bus. & Com. Code § 17.45(3).

68. Flagstar advertised, offered, or sold goods or services in Texas and engaged in trade or commerce directly or indirectly affecting the people of Texas, as defined by Tex. Bus. & Com. Code § 17.45(6).

69. Flagstar engaged in false, misleading, or deceptive acts and practices in violation of Tex. Bus. & Com. Code § 17.46(b), including:

a. Representing that goods or services had sponsorship, approval, characteristics, ingredients, uses, benefits, or quantities that they did not have;

b. Representing that goods or services were of a particular standard, quality, or grade, when they were of another; and

c. Advertising goods or services with intent not to sell them as advertised.

70. Flagstar's false, misleading, or deceptive acts and practices include:

a. Failing to have reasonable data security measures in place to protect Plaintiff's Private Information, which was a direct and proximate cause of the Data Breach;

b. Failing to identify foreseeable security and privacy risks, remediate identified security and privacy risks, and adequately improve security and privacy measures following previous cybersecurity incidents, which was a direct and proximate cause of the Data Breach;

c. Failing to comply with common law and statutory duties pertaining to the security and privacy of Plaintiff's' Private Information, including duties imposed by the FTC Act, 15 U.S.C. § 45 and Texas's data security statute, Tex. Bus. & Com. Code § 521.052, which was a direct and proximate cause of the Data Breach;

d. Failing to timely and adequately notify Plaintiff of the Data breach;

e. Misrepresenting that it would protect the confidentiality and privacy of Plaintiff's Private Information, including by implementing and maintaining reasonable security measures;

f. Misrepresenting that certain sensitive Personal Information was not accessed during the Data Breach; and

g. Omitting, suppressing, and concealing the material fact that it did not reasonably or adequately secure Plaintiff's Private information.

71. Flagstar's representations and omissions were material because they were likely to deceive reasonable consumers regarding the adequacy of Flagstar's data security. The representations and omissions were also material because they were likely to deceive reasonable consumers that their Private Information was not exposed, misleading Plaintiff into believing he did not need to take action to protect or monitor his identity.

72. Flagstar intended to mislead Plaintiff and Class Members and induce them to rely on its omissions and misrepresentations.

73. Class members' substantial injuries are a direct and proximate result of Defendant's misrepresentations and omissions. Plaintiff and Class Members have suffered and will continue to suffer injury, ascertainable loss of money or property, and monetary and non-monetary damages including from identity theft and fraud; time and expenses related to monitoring their accounts for fraudulent activity; loss of value of Private Information; and an increased risk of identity theft and fraud.

74. Plaintiff and Class members seek all monetary and non-monetary relief allowed by law, including economic damages; damages for mental anguish; treble damages for each act committed intentionally or knowingly; court costs; reasonably and necessary attorneys' fees; injunctive relief; and any other relief which the court deems proper.

PRAYER FOR RELIEF

Wherefore, Plaintiff respectfully requests that the Court enter an order of judgment that:

1. Certifies this action as a class action and appoints Plaintiff as class representative and the undersigned counsel as class counsel;

2. Awards actual damages, compensatory damages, statutory damages, and statutory penalties in an amount to be determined, as allowable by law;

3. Awards pre- and post-judgment interest at the maximum allowable rates on any amounts awarded

4. Awards appropriate injunctive and equitable relief;

5. Awards reasonable attorneys' fees and costs, and any other expense, including reasonable expert witness fees; and

6. Orders any further relief that this Court deems just and proper.

DEMAND FOR JURY TRIAL

Plaintiff hereby demands trial by jury.

Dated: November 7, 2022

Respectfully submitted,

/s/ Gretchen Freeman Cappio
Gretchen Freeman Cappio, (P84390)
Ryan P. McDevitt, (P84389)
Sydney Read
KELLER ROHRBACK L.L.P.
1201 Third Avenue, Suite 3200
Seattle, WA 98101-3052
Telephone: (206) 623-1900
Fax: (206) 623-3384
gcappio@kellerrohrback.com
rmcdevitt@kellerrohrback.com
sread@kellerrohrback.com

E. Powell Miller (P39487)
Sharon S. Almonrode (P33938)
THE MILLER FIRM, P.C.
Miller Building
950 West University Drive, Suite 300
Rochester, MI 48307
Telephone: (248) 841-2200
Fax: (248) 652-2852
epm@millerlawpc.com
ssa@millerlawpc.com

Joseph H. Meltzer
Melissa L. Troutner
Ethan J. Barlieb
KESSLER TOPAZ
MELTZER & CHECK, LLP
280 King of Prussia Road
Radnor, PA 19087
Telephone: (610) 667-7706
Fax: (610) 667-7056
jmeltzer@ktmc.com
mtroutner@ktmc.com
ebarlieb@ktmc.com

4889-7541-3806, v. 6